



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
|-----------------|-------------|----------------------|---------------------|------------------|

09/710,203

11/09/2000

Hideki Koike

LEXW116493

4596

26389

7590

03/22/2006

CHRISTENSEN, O'CONNOR, JOHNSON, KINDNESS, PLLC
1420 FIFTH AVENUE
SUITE 2800
SEATTLE, WA 98101-2347

EXAMINER

ABRISHAMKAR, KAVEH

ART UNIT

PAPER NUMBER

2131

DATE MAILED: 03/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/710,203

Applicant(s)

KOIKE ET AL.

Examiner

Kaveh Abrishamkar

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 19 December 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-6,8-21, and 23- 26 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-6,8-21, and 23- 26 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: _____

DETAILED ACTION

1. In view of the Appeal Brief filed on December 19, 2005, PROSECUTION IS HEREBY REOPENED. A new grounds of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

2. Claims 1-26 are currently being considered.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Art Unit: 2131

3. Claims 1-26 are rejected under 35 U.S.C. 102(a) as being anticipated by Schneier et al. ("Cryptographic Support for Secure Logs on Untrusted Machines").

Regarding claim 1, Schneier discloses:

A log file protection system for protecting log files in which computer system operations have been recorded, comprising:

log file creation means which create a plurality of identical log files which record the operations of said computer systems (Section 3.2: paragraph 1; Section 4.2: paragraphs 8-11), wherein it is stated that "U_o should log the data in several parallel logfiles, with each logfile using a different untrusted server as its trusted server";

alteration detection means which periodically monitor said plurality of identical log files for alteration or deletion (Section 1: paragraphs 4, 9-11, Section 3.3: paragraph 1; Section 3.4: paragraph 1); and

restoration means which restore the altered or deleted log file by replacing the altered or deleted log file with an unaltered log file from the plurality of identical log files when the altered or deleted log file is detected by said alteration detection means (Section 5: paragraph 1), wherein the log file can be replaced with a clean backup.

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Schneier discloses:

The log file protection system of claim 1, wherein said log file creation means create said plurality of identical log files in parallel, using identical information (Section 4.2: paragraphs 8-11).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Schneier discloses:

The log file protection system of claim 1, further comprising hiding means which hide all but one of the plurality of log files (Section 2: paragraph 14), wherein all the parallel log files are stored in other locations other than the primary untrusted computer.

Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Schneier discloses:

The log file protection system of claim 3, wherein said hiding means periodically re-hide said hidden log files in different locations (Section 5: paragraph 1), wherein the log file can be replaced with a clean backup, which is moving the hidden log file to the untrusted machine.

Claim 5 is rejected as applied above in rejecting claim 3. Furthermore, Schneier discloses:

The log file protection system of claim 3, wherein said hiding means re-hide said hidden log files in different locations, when alteration or deletion is detected by said alteration detection means (Section 5: paragraph 1), wherein the log file can be

Art Unit: 2131

replaced with a clean backup, which is moving the hidden log file to the untrusted machine.

Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, Schneier discloses:

The log file protection system of claim 5, further comprising means which perform additional processing, when alteration or deletion is detected by said alteration detection means (Section 5: paragraph 1), wherein the log file can be replaced with a clean backup, which is moving the hidden log file to the untrusted machine.

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Schneier discloses:

The log file protection system of claim 1, further comprising means which perform additional processing when alteration or deletion is detected by said alteration detection means (Section 5: paragraph 1), wherein the log file can be replaced with a clean backup, which is moving the hidden log file to the untrusted machine.

Claim 9 is rejected as applied above in rejecting claim 2. Furthermore, Schneier discloses:

The log file protection system of claim 2, further comprising means which perform additional processing when alteration or deletion is detected by said alteration detection

Art Unit: 2131

means (Section 5: paragraph 1), wherein the log file can be replaced with a clean backup, which is moving the hidden log file to the untrusted machine.

Claim 10 is rejected as applied above in rejecting claim 2. Furthermore, Schneier discloses:

The log file protection system of claim 2, further comprising hiding means which hide all but one of the plurality of identical log files (Section 2: paragraph 14), wherein all the parallel log files are stored in other locations other than the primary untrusted computer.

Claim 11 is rejected as applied above in rejecting claim 10. Furthermore, Schneier discloses:

The log file protection system of claim 10, further comprising means which perform additional processing when alteration or deletion is detected by said alteration detection means (Section 5: paragraph 1), wherein the log file can be replaced with a clean backup, which is moving the hidden log file to the untrusted machine.

Claim 12 is rejected as applied above in rejecting claim 10. Furthermore, Schneier discloses:

The log file protection system of claim 10, wherein said hiding means re-hide said hidden log files in different locations, when alteration or deletion is detected by said alteration detection means (Section 5: paragraph 1), wherein the log file can be

Art Unit: 2131

replaced with a clean backup, which is moving the hidden log file to the untrusted machine.

Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Schneier discloses:

The log file protection system of claim 12, further comprising means which perform additional processing when alteration or deletion is detected by said alteration detection means (Section 5: paragraph 1), wherein the log file can be replaced with a clean backup, which is moving the hidden log file to the untrusted machine.

Claim 14 is rejected as applied above in rejecting claim 10. Furthermore, Schneier discloses:

The log file protection system of claim 10, wherein said hiding means periodically re-hide said hidden log files in different locations (Section 5: paragraph 1), wherein the log file can be replaced with a clean backup, which is moving the hidden log file to the untrusted machine.

Claim 15 is rejected as applied above in rejecting claim 14. Furthermore, Schneier discloses:

The log file protection system of claim 14, further comprising means which perform additional processing when alteration or deletion is detected by said alteration

Art Unit: 2131

detection means (Section 5: paragraph 1), wherein the log file can be replaced with a clean backup, which is moving the hidden log file to the untrusted machine.

Claim 16 is rejected as applied above in rejecting claim 14. Furthermore, Schneier discloses:

The log file protection system of claim 14, wherein said hiding means periodically re-hide said hidden log files in different locations (Section 5: paragraph 1), wherein the log file can be replaced with a clean backup, which is moving the hidden log file to the untrusted machine.

Claim 17 is rejected as applied above in rejecting claim 16. Furthermore, Schneier discloses:

The log file protection system of claim 16, further comprising means which perform additional processing when alteration or deletion is detected by said alteration detection means (Section 5: paragraph 1), wherein the log file can be replaced with a clean backup, which is moving the hidden log file to the untrusted machine.

Claim 18 is rejected as applied above in rejecting claim 3. Furthermore, Schneier discloses:

The log file protection system of claim 3, further comprising means which perform additional processing when alteration or deletion is detected by said alteration detection

Art Unit: 2131

means (Section 5: paragraph 1), wherein the log file can be replaced with a clean backup, which is moving the hidden log file to the untrusted machine.

Claim 19 is rejected as applied above in rejecting claim 4. Furthermore, Schneier discloses:

The log file protection system of claim 4, further comprising means which perform additional processing when alteration or deletion is detected by said alteration detection means (Section 5: paragraph 1), wherein the log file can be replaced with a clean backup, which is moving the hidden log file to the untrusted machine.

Claim 20 is rejected as applied above in rejecting claim 4. Furthermore, Schneier discloses:

The log file protection system of claim 4, wherein said hiding means periodically re-hide said hidden log files in different locations (Section 5: paragraph 1), wherein the log file can be replaced with a clean backup, which is moving the hidden log file to the untrusted machine.

Claim 21 is rejected as applied above in rejecting claim 20. Furthermore, Schneier discloses:

The log file protection system of claim 20, further comprising means which perform additional processing when alteration or deletion is detected by said alteration

Art Unit: 2131

detection means (Section 5: paragraph 1), wherein the log file can be replaced with a clean backup, which is moving the hidden log file to the untrusted machine.

Claim 23 is rejected as applied above in rejecting claim 1. Furthermore, Schneier discloses:

The log file protection system of claim 1, wherein said alteration detection means monitor said log files by using fingerprint data generated based on the entire content of the log file (Section 3: paragraph 5; Section 3.4: paragraph 1; Section 3.5: paragraph 3).

Claim 24 is rejected as applied above in rejecting claim 1. Furthermore, Schneier discloses:

The log file protection system of claim 1, wherein said alteration detection means monitor said log files by using fingerprint data generated based on the entire content of the log file (Section 5: paragraph 1).

Regarding claim 25, Schneier discloses:

Recording media which stores a program capable of implementing the log file protection system according to any of Claims 1-6,8-21, or 23-24 on a computer system (Section 1: paragraphs 4, 9-11, Section 3.3: paragraph 1; Section 3.4: paragraph 1; Section 5: paragraph 1).

Regarding claim 26, Schneier discloses:

A log file protection method for protecting log files in which computer system operations have been recorded, comprising:

(a) creating a plurality of identical log files which record the operations of said computer system systems (Section 3.2: paragraph 1; Section 4.2: paragraphs 8-11), wherein it is stated that "U_o should log the data in several parallel logfiles, with each logfile using a different untrusted server as its trusted server";

(b) periodically monitoring said plurality of identical log files for alteration or deletion (Section 1: paragraphs 4, 9-11, Section 3.3: paragraph 1; Section 3.4: paragraph 1); and

(c) restoring the altered or deleted log file by replacing the altered or deleted log file with an unaltered log file from the plurality of identical log files when the altered or deleted log file is detected in said periodic monitoring step (Section 5: paragraph 1), wherein the log file can be replaced with a clean backup.


Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

 3/19/06

KA
03/18/2006

CHRISTOPHER REVAK
PRIMARY EXAMINER